ALB:MEF
F.# 2019R00857

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF: (1) ONE IPAD MODEL A1823, SERIAL NUMBER F9FT51T5HLJJ; (2) ONE IPAD MODEL A1475, SERIAL NUMBER DMPM3BPMF4YJ; (3) ONE SONY CAMERA, SERIAL NUMBER 1122050; (4) ONE SANDISK 4G SD CARD, SERIAL NUMBER BH1026516075G; AND (5) ONE BLACK IPHONE X.	**TO BE FILED UNDER SEAL** APPLICATION FOR A SEARCH WARRANT FOR ELECTRONIC DEVICES Case No. MJ - 19 545

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, DANIEL FANDREY, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—tablets, a digital camera, an SD CARD and a cellular phone—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Task Force Officer with the Federal Bureau of Investigation ("FBI") and a Detective with the Suffolk County Police Department. I have been employed as a Task Force Officer since 2017, as a Detective since 2016 and as a Police Officer since 2007. I am currently assigned to the Child Exploitation and Human Trafficking Task Force (the "Task Force"). The Task Force investigates individuals suspected of being involved in the online

sexual exploitation of children. While on the Task Force, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation and child pornography. As part of my duties, I investigate violations relating to child exploitation and child pornography, including violations pertaining to the production, possession, distribution, and receipt of child pornography as well as the transportation of minors and interstate travel to engage in illicit sexual conduct, in violation of Title 18, United States Code, Sections 2251, 2252, 2252A, and 2423. I have received training in the area of child pornography and child exploitation, and I have had the opportunity to observe and review numerous examples of child pornography (as defined below) in all forms of media, including computer media. As a Task Force Officer, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

3. The statements in this affidavit are based on my own investigation of this matter, in addition to information provided to me by Special Agents of the FBI and other members of the Task Force. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched is: (1) ONE IPAD MODEL A1823, SERIAL NUMBER F9FT51T5HLJJ ("Device 1"); (2) ONE IPAD MODEL A1475, SERIAL NUMBER DMPM3BPMF4YJ ("Device 2"); (3) ONE SONY CAMERA, SERIAL NUMBER 1122050 ("Device 3"); (4) ONE SANDISK 4G SD CARD, SERIAL NUMBER BH1026516075G ("Device 4"); AND (5) ONE BLACK IPHONE X ("Device 5"),

(collectively, the "Devices"). The Devices are currently in FBI custody in the Eastern District of New York.

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

DEFINITIONS

6. For the purposes of the requested warrant, the following terms have the indicated meaning in this affidavit:

a. The terms "minor," "sexually explicit conduct" and "visual depiction," are defined as set forth in Title 18, United States Code, Section 2256.

b. The term "child pornography" is defined in Title 18, United States Code, Section 2256(8) in pertinent part as "any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where . . . the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct . . . or (C) such visual

depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.""[1]

PROBABLE CAUSE

7. On or about May 2, 2019, the FBI received information in connection with an ongoing investigation of Kik group chats regarding a Kik chat room identified as "dad4dau." One of the Kik "dad4dau" chat room users identified during the investigation had the display name "Josh Smith" and the user name "joshjamie516" (the "Josh Smith Account"). On April 26, 2019, the Josh Smith Account posted to the "dad4dau" chat room the following: "dad here with daughter – any others?pm".

8. On or about April 26, 2019, a law enforcement officer working in an undercover capacity (the "UC") sent the Josh Smith Account a private message via Kik, which stated that the UC was also the father of a nine-year-old daughter and a seven-year-old son. The Josh Smith Account responded that his daughter was "14 and we play" and that sexual interactions with his daughter included "touching and handjob." The Josh Smith Account also sent the UC non-pornographic photographic images via Kik, which were alleged to be of his daughter. The Josh Smith Account is associated with the email address joshjamie516@gmail.com and IP address 173.68.184.34. According to information obtained from Verizon Fios, the subscriber for this IP address, when used by the Kik account from

---

[1] See also Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002) (analyzing constitutional validity of the definitions set forth in 18 U.S.C. § 2256(8)).

April 2, 2019 to April 27, 2019, was Brett Ofsink ("Ofsink"), who resides at a residence in Syosset, New York. An email address attached to the IP address also included Ofsink's first and last name.

9. On or about May 31, 2019, I, along with FBI Special Agent Cindy Wolf, interviewed Offsink immediately outside of his Syosset residence. During the course of the interview, Ofsink stated that he had used Kik on his desktop computer through a program called BlueStacks. Ofsink further recalled being in a Kik chat room about dads and daughters and that his user name was "Josh James." Ofsink also identified the photographic image that he had sent to the UC, which Ofsink indicated was not of his daughter but downloaded from the internet.

10. At the time of the interview, Ofsink gave his written consent to allow the FBI to perform a forensic search of his computer HP computer, which Ofsink gave to the FBI (the "HP Computer").

11. On or about May 31, 2019, the FBI conducted a forensic examination of the HP Computer. In addition to recovering the photographic images Ofsink sent to the UC, the FBI recovered images and videos of child pornography from a folder titled "BlueStacks." More specifically, contained within the "BlueStacks" folder were, among others, the following videos, which are available for the Court's review:

a. a video approximately 74 seconds in length depicting a female toddler naked from the waist down being anally penetrated by an adult male's penis;

b. a video approximately 63 seconds in length depicting a male toddler naked from the waist down penetrating an adult female vaginally with his penis. The adult female is holding the toddler by his buttocks while simultaneously spreading the toddler's buttocks and exposing his anus to the camera; and

c. a video approximately 10 seconds in length depicting a naked prepubescent female being anally penetrated by an adult male's penis.

12. As part of the forensic analysis of the HP Computer, I also recovered:

a. images of Ofsink's daughter, who is currently 11 years old, but who was 2 to 3 years younger at the time, posing in a bikini with one leg over her head (with her face blocked out using computer software);

b. recent images of Ofsink's 11-year-old daughter in a bikini, standing beside Ofsink's wife, who is topless, in a bathroom, which, based on an interview of Ofsink's wife, were taken without their knowledge;

c. numerous nude images of Ofsink's wife, in locations including her bedroom and bathroom, which, based on an interview of Ofsink's wife, were taken without her knowledge (together with (a) and (b), the "Sexual Family Photos");

d. numerous non-pornographic images of Ofsink's 11 year-old daughter, where she ranges in age from approximately 9 to 11 years old (with her face blocked out using computer software);

e. the text of chats between Ofsink and other unknown online users, wherein they discuss incestual acts on children and the exchange of unknown images, which appear to have been distributed and received during these chats.

13. According to my forensic review of the HP Computer, the Sexual Family Photos were originally taken using either an iPhone, a Sony Camera and an iPad. Additionally, at some earlier date, an SD card had been plugged into the HP Computer.

14. On, June 6, 2019, the Honorable Gary R. Brown, United States Magistrate Judge, signed a complaint charging Ofsink with violating 18 U.S.C. § 2252(a)(2) (receipt of child pornography), and issued a warrant for Ofsink's arrest (No. 19-MJ-530).

15. On June 7, 2019, I, along with other members of the Task Force, placed Ofsink under arrest in connection with the aforementioned warrant. The arrest took place several blocks from Ofsink's home. At the time of this arrest, Ofsink had Device 4, the black iPhone X, on his person.

16. Thereafter, members of the Task Force went to Ofsink's home, where they interviewed Ofsink's wife, and confirmed that the aforementioned Sexual Family Photos were taken without her knowledge. Present in the home was Ofsink's 11-year-old daughter. At that time, and based on the results of the forensic analysis of the HP Computer, members of the Task Force asked Ofsink's wife if they could review any iPads, Sony Cameras or SD cards that belonged to Ofsink. At that time, Ofsink's wife voluntarily gave Device 1, Device 2 and Device 3, which contained Device 4, to members of the Task Force. Ofsink's wife informed the Task Force members that these devices all belonged to Ofsink.

17. After Ofsink was in custody, I read him his Miranda rights, which he agreed to waive both orally and in writing. Thereafter, Ofsink stated in sum and substance that, for approximately one year, he had utilized Kik to access different [chat] rooms, some of which had child pornography; he has been in chats where he has discussed sexual acts with kids, including both other people's children and his own; he has asked for, sent and received images and videos of children; on Kik, he utilizes the screenname "Joshjamie516"; and he also is interested in porn that involves "wife stuff." Ofsink also signed a written statement that contained this information.

TECHNICAL TERMS

18. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video;

storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the

ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards

or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, which is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers

have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

19. Based on my training, experience and research, I know that Device 1, Device 2, Device 3 and Device 5 have capabilities that allow them to serve as a digital camera. Additionally, Device 1, Device 2 and Device 5 can serve as a portable media player, PDA, wireless telephone, and GPS navigation device. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

20. Based on my training, experience and research, I know that Device 3, the Sony Camera, is capable of storing digital images in its memory, apart from any SD card contained inside of it. Additionally, Device 4, the SD card, is capable of storing digital images, which can then be viewed by connecting the card to a variety of electronic devices, including but not limited to cameras or personal computers.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because

special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

22. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

23. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record

additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

25. *Manner of execution.* Because this warrant seeks only permission to examine Devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY

26. Based on my training and experience and conversations that I have had with other federal agents and law enforcement offices, I know that child pornography is not readily available in retail establishments. Accordingly, individuals who wish to obtain child pornography do so usually by ordering it from abroad or by discreet contact, including through the use of the Internet, with other individuals who have it available or by accessing web sites containing child pornography. Child pornography collectors often send and receive electronic mail conversing with other collectors in order to solicit and receive child pornography.

27. I have learned that collectors of child pornography typically retain their materials and related information for many years.

28. I have learned that collectors of child pornography typically transfer their materials between and among electronic devices with ease, which they may do through the use of external hard drives, memory cards or cloud features, to name a few.

29. I also have learned that collectors of child pornography often maintain lists of names, addresses, telephone numbers and screen names or individuals with whom they have been in contact and who share the same interests in child pornography.

30. Accordingly, information in support of probable cause in child pornography cases is less likely to be stale because collectors and traders of child pornography are known to store and retain their collections and correspondence with other collectors and distributors for extended periods of time.

31. Further, based on my training, knowledge, expertise and discussions with other law enforcement officers, I understand that, in the course of executing a search warrant for the possession, transportation, receipt, distribution or reproduction of sexually explicit material related to children, on numerous occasions officers have recovered evidence related to the production of child pornography and/or child exploitation.

32. Based upon my training, experience and the investigation to date, as described above, particularly the recovery of child pornography images from the HP Computer, along with surreptitiously created nude images of Ofsink's wife, coupled with the images of Ofsink's daughter with her face blurred out, I believe that Ofsink is a collector of child pornography and that it is likely that the Devices contain child pornography images and evidence relating to child pornography images and trading.

CONCLUSION

33. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

REQUEST FOR SEALING

34. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into child pornography. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a

significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

DANIEL FANDREY
Task Force Officer
FEDERAL BUREAU OF
INVESTIGATION

Subscribed and sworn to before me
on June 14, 2019

/S/ STEVEN I. LOCKE
HO
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

The property to be searched is: (1) ONE IPAD MODEL A1823, SERIAL NUMBER F9FT51T5HLJJ; (2) ONE IPAD MODEL A1475, SERIAL NUMBER DMPM3BPMF4YJ; (3) ONE SONY CAMERA, SERIAL NUMBER 1122050; (4) ONE SANDISK 4G SD CARD, SERIAL NUMBER BH1026516075G; AND (5) ONE BLACK IPHONE X, hereinafter the "Devices."

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A constituting evidence or instrumentalities of the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2251, 2252 and 2252A:

a. Images of child pornography and files containing images of child pornography and records, images, information or correspondence pertaining to the possession, access with intent to view, receipt or distribution of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2251, 2552 and 2552A, in any form wherever they may be stored or found;

b. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

c. Records, information, or correspondence pertaining to the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, as defined in Title 18, United States Code, Section 2256, including but not limited to:

i. Correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors

engaged in sexually explicit conduct, as defined by Title 18, United States Code, Section 2256; and

ii. Records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or computer of any visual depiction of minors engaged in sexually explicit conduct, as defined by Title 18, United States Code, Section 2256;

2. All nude or semi-nude photographs of children, including but not limited to Ofsink's own children;

3. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.